Magic Quadrant for Unified Threat Management

7 August 2014 ID:G00261973

Analyst(s): Jeremy D'Hoinne, Adam Hils, Greg Young

VIEW SUMMARY

Unified threat management devices provide small and midsize businesses with multiple network security functions in a single appliance. Buyers should focus on performance when many security functions are enabled, and on the skill set of the associated channel partner.

Market Definition/Description

Gartner defines the unified threat management (UTM) market as multifunction network security products used by small or midsize businesses (SMBs). Typically, midsize businesses have 100 to 1,000 employees (see Note 1). UTM products must continually add new functions and therefore encompass the feature set of many other network security solutions including next-generation firewall, secure Web gateway and secure email gateway. While consolidation comes with compromises in performance and capability, these are compromises that many SMBs are willing to accept (see "What You Should Expect From Unified Threat Management Solutions").

Many UTM products contain various other security capabilities, such as wireless option and modular Ethernet port density, and, less frequently, Web application firewa (WAF) and data loss prevention (DLP) software modules. Application control embedded in UTM is often basic, focused on Internet applications (Facebook, Google applications, YouTube) and loosely integrated with the filtering policy through a list of applications bundled in a profile and attached to the filtering rule. It is used mostly to restrict the use of Web applications and cloud services (such as social media, file sharing and so on). Features related to the management of mobile devices create a potentially attractive differentiator for this market (see "How Unified Threat Management Tackles the Consumerization of IT").

UTM appliances are used by midsize businesses to meet the requirements for secure Internet connectivity. For many small businesses, those requirements are often driven by regulatory demands (such as the PCI Data Security Standard), mandating rudimentary levels of security controls. Browser-based management, basic embedded reporting, and localized software and documentation, which don't specifically appeal to large enterprises are highly valued by SMBs in this market. Gartner sees very different demands from the enterprise and branch office firewall markets (see "Magic Quadrant for Enterprise Network Firewalls"), which generally require more-complex network security features, and are optimized for very different selection criteria.

The branch offices of larger companies have very different network security demand from midsize businesses, even though they may be of similar size. Gartner views branch offices' firewalls as extensions of the central firewall strategy (see "Bring Branch Office Network Security Up to the Enterprise Standard"). This drives large enterprises to often use low-end enterprise products at their branch offices to ensure interoperability, and to take advantage of economies of scale in getting larger discounts from their firewall vendors. For these reasons, Gartner allocates branch office firewall revenue to the enterprise firewall market, not the UTM market.

For 2013, Gartner estimates that the UTM market grew at 14.1% to reach a total cap approximately $1.54 billion (see "Market Share Analysis: Unified Threat Management (SMB Multifunction Firewalls), Worldwide, 2014 Update" and Note 2).

Many UTM vendors, which put a strong focus on distributed organizations such as retai or managed security service providers (MSSPs), are now heading toward placing the management and monitoring consoles fully in the cloud. Gartner believes that, although it's convenient for the vendors to do so, a portion of the SMB market will not accept this exclusively cloud model for reasons of latency, and need to access the console when under attack. In some regions and industry verticals, limited trust in a foreign supplier and other privacy concerns would be additional reasons to avoid the cloud model. Reporting and log retention are well-suited to the cloud, but not exclusively.

SMBs should be skeptical of the aspirational message from UTM vendors about the exaggerated benefits of feature consolidation. Security buyers should instead evaluate UTM device based on the controls they will actually use, the performance they will get for those features, and the quality of vendor and channel (and managed services) support that is available.

The market for network and security solutions designed to protect SMBs continues to develop, and our expectations for UTM technology features increase with each new edition of this Magic Quadrant. As a result, the Magic Quadrant depicts a shift up and to the right with each revision. Consequently, vendors must progress to maintain their positions in each new Magic Quadrant.

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management

STRATEGIC PLANNING ASSUMPTIONS

Replacement of UTM by cloud options will remain at less than 5% through 2016; however, by then, most UTM devices will leverage cloud-assisted security or management features.

By 2016, 15% of SMBs will use mobility management capabilities from their UTM platforms to enforce distinctive policies — up from less than 5% today.

NOTE 1
SMALL AND MIDSIZE MARKET DEFINITION

Gartner generally defines SMBs by the number of employees and/or annual revenue they have. The primary attribute that is used most often is the number of employees. Small businesses usually have fewer than 100 employees, while midsize businesses are usually defined as companies with fewer than 1,000 employees. The secondary attribute that is used most often is annual revenue. Small businesses are usually defined as those with less than $50 million in annual revenue, while midsize businesses are defined as those with less than $1 billion in annual revenue. Typically, 80% of the companies that Gartner analysts speak with have between 100 and 999 employees, and revenue of $100 million to $500 million (see "Gartner's Small and Midsize Business Market Definition, 2013 Update").

NOTE 2
UTM REVENUE DIFFERENTIATION

Gartner does not include branch office firewall revenue as UTM revenue. The market size and growth are estimated compared with numbers from the previous UTM Magic Quadrant.

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

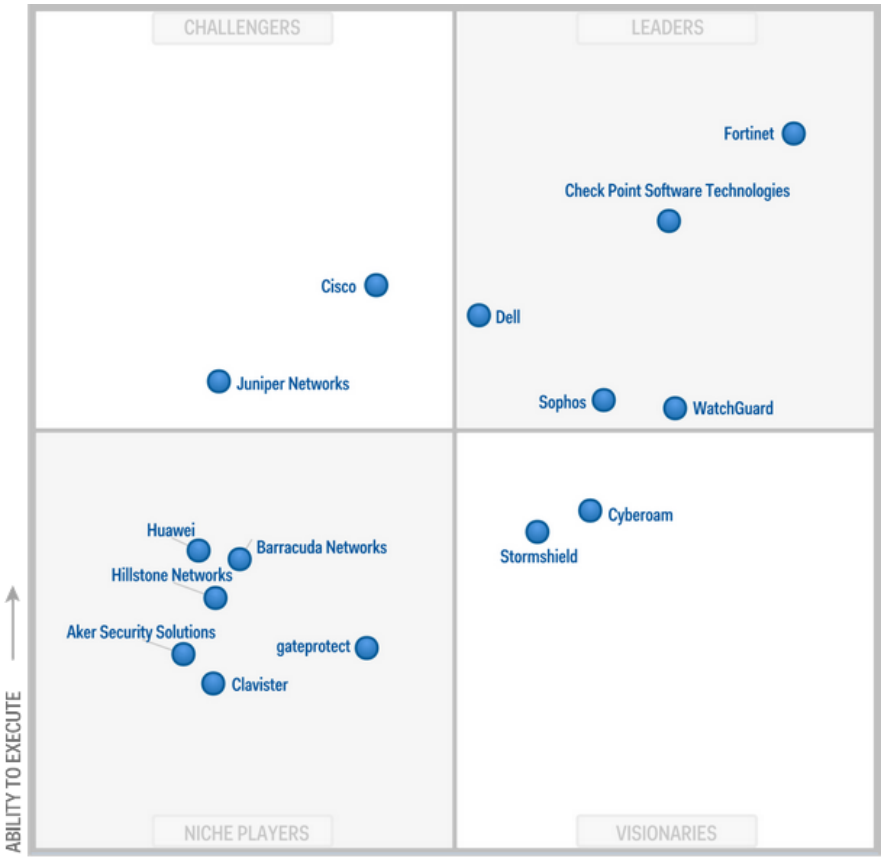
Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems



Source: Gartner (August 2014)

Vendor Strengths and Cautions

Aker Security Solutions

Based in Brazil, Aker Security Solutions is a network security vendor. Its portfolio has included UTM solutions (Aker Firewall UTM) since 1997, as well as secure Web gateway and secure email gateway. Aker Firewall UTM is composed of 14 models, with two models with wireless capabilities. It can also run as a virtual appliance on VMware, Citrix Xen and Microsoft Hyper-V.

In the past 12 months, Aker renewed its entire hardware appliance product line and added Kaspersky Anti-Virus as an option.

Aker Firewall UTM is a good shortlist candidate for small and midsize organizations in Brazil.

Strengths

- Aker Firewall UTM provides a comprehensive set of UTM features, including application control, wireless security, SSL VPN, and two choices each for an antivirus engine and an intrusion prevention system (IPS) signature set.
- Aker provides a rental option for its UTM appliances, which reduces capital expenditure (capex) costs.
- Aker's clients and its channel partners value the availability of 24/7 vendor support.
- Aker is one of the few vendors that provide graphical user interface (GUI), documentation and support in Portuguese.

Cautions

- Aker Firewall UTM lacks a low-end appliance (less than $1,000) that could be cost-effective for small offices.
- Aker does not provide an embedded Web interface, but instead always requires the installation of a management software component (Aker Control Center). Clients report that installation could be easier.
- Aker is not visible in client shortlists outside of Brazil, and is not ready for internationalization yet.

Barracuda Networks

Based in Campbell, California, Barracuda Networks is a large vendor providing network security, backup and infrastructure solutions, including, among other things, Web and email security, Web application firewall, and data backup. It has a strong focus on SMBs, but until recently was lacking a dedicated UTM offering. In February 2013, Barracuda released a new product line, the Barracuda Firewall (X series), to complement Barracuda NG Firewall (F series), its incumbent range of firewalls, which are oriented toward larger enterprises' needs. Barracuda Firewall is composed of seven models, including two with wireless capabilities, but is not available yet as a virtual appliance. It embeds a Web interface, designed for simpler use cases, and leverages cloud databases and engines for key content filtering.

At the end of 2013, Barracuda executed an initial public offering (IPO). In the past few months, it expanded the Barracuda Firewall product ranges toward smaller offices and added software features to ease the installation process.

and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

The Barracuda Firewall series is a good shortlist candidate for SMBs that already use other Barracuda products, have an existing trustful relationship with resellers of Barracuda solutions or have stringent budget constraints.

Strengths

- Barracuda has strong market share among SMBs, and customers benefit from good global sales and support presence, especially in Europe.
- Gartner clients report that they like the simple licensing, and that unlike many competitors, the price for software options is reasonable.
- Barracuda Networks offers a 30-day refund plan and a replacement program that includes a new appliance every four years.

Cautions

- The Barracuda X Series was only recently released; some integrated modules and the cloud-based centralized management are yet unproven. Barracuda's channel is unevenly trained on the solution in some regions.
- The Barracuda X Series has not been scrutinized by any major third-party testing labs and has a limited number of certifications.
- Gartner believes that, while Barracuda has correctly assessed that SMB and enterprise have different needs, customers and channel partners could be confused because the two firewall lines have more overlaps than differences.

Check Point Software Technologies

Check Point Software Technologies, with headquarters in Tel Aviv, Israel, and San Carlos, California, is one of the largest pure-play security companies, and has been present in the security market for more than 20 years. Initially exclusively focused on enterprises, Check Point has later invested in the UTM segment, specifically targeting SMB use cases. Its SMB product line includes 11 appliances, including wireless and DSL models. UTM can also be delivered as a virtual appliance or on Amazon Web Services (AWS). Fundamental to Check Point firewall offerings is the set of software options referred to as Software Blades that can be grouped together in bundles.

Once the hardware and OS consolidation work was achieved in 2013, Check Point moved its efforts back to new threat prevention features and performance improvements. It has also recently made available a marketplace of threat feeds from third parties that its clients can purchase separately as software options (ThreatCloud IntelliStore).

Check Point is a good choice for SMB organizations that do not consider low price as the most important criterion.

Strengths

- Check Point's reporting and management console is consistently highly rated by midsize companies. Check Point managed to simplify its management console for its entry level appliances without compromising the flexibility and depth of protection.
- Check Point's UTM solutions benefit from its enterprise-level security features, such as ThreatCloud and Anti-Bot software options, in addition to the strong IPS module, which are all backed up by Check Point's large threat research team.
- Check Point provides an option for sandboxing (Threat Emulation), and recently released a cloud-based security service for mobile and remote users, in addition to having existing partnerships with mobile device management (MDM) solutions.
- Check Point is a strong, stable organization with a consistent strategy and proven ability to execute on its road map.

Cautions

- Gartner sees Check Point mostly selling to its existing base of distributed enterprises, but it does lag behind other Leaders in building a dedicated channel of purely SMB resellers.
- Gartner clients often cite price as the primary reason for not selecting Check Point solutions.
- Gartner SMB clients report that the quality of Level 1 support from channel varies, and Gartner has observed that SMB customer problem escalations take more time to resolve than those from large enterprise customers.
- Check Point offers many Software Blades and keeps adding new ones. It has made good progress in simplifying the sales offering with bundles, but resellers and clients report that they find it difficult to assess the overall impact of enabling more than a few options simultaneously.

Cisco

Cisco, based in San Jose, California, is the largest network infrastructure provider. For a long time, it used its global presence to cross-sell security solutions to its existing customer base. Cisco now dedicates renewed efforts to the enterprise security market with the acquisition of Sourcefire in 2013, and focuses on security for distributed SMBs with cloud-managed Meraki MX appliances (seven models). Its portfolio still provide the ISA500 Series for small businesses (four models, including two with wireless capabilities), and the ASA 5500-X Series for midsize companies (five models). Cisco Adaptivity Security Appliance (ASA) is also available as a virtual appliance (ASAv). In addition to the dedicated security solutions, Cisco has a large portfolio of network solutions that can provide security features, such as Integrated Services Routers (ISRs).

During the past 12 months, Cisco predominantly promoted and improved its Meraki MX product line with the integration of Sourcefire IPS and the addition of user identity filtering capabilities.

Cisco is a good choice for existing SMB customers using other Cisco technology, and for distributed organizations in North America.

Strengths

- Cisco's Gartner customers generally offer positive reviews of Cisco hardware robustness.

The learning curve for Cisco trained staff on its security technology is short, especiallfor customers already familiar with the Cisco command line interface.

Cisco Meraki MX includes contextual feeds from Sourcefire, integrated Wi-Fi/4G management, and integration with MDM solutions for mobile users.

Cisco Meraki MX cloud-based centralized management offers a unified view for managing UTMs, Meraki's wireless AP and switches. Customers can create configuration templateto add new locations and to create site-to-site VPN more easily.

Cautions

Cisco Meraki MX lacks email security, SSL VPN for remote users and SSL decryptiorfor HTTP that are available in many of its competitors' UTMs.

Cisco's dual product line strategy for the UTM market might create complexity fosome clients that could leverage their Cisco knowledge with Cisco ASA on the corenetwork, but could also benefit from some of the Meraki MX features for distributecoffices.

Cisco does not generate many inquiries from SMB clients, and when it does, it is oftethe incumbent solution that is considered for replacement.

Clavister

Clavister, headquartered in Sweden, primarily targets enterprises and ISPs with its applianceand cloud services. The vendor addresses SMBs through its branded security appliancesthe Eagle Series and the Wolf Series, that can be delivered as virtual appliancestoo. Its operating system (cOS) is provided either as a full-fledged software stack(cOS Core) or as a streamlined version focused on network needs (cOS Stream). Clavisteralso offers a dedicated portal to MSSPs for the management of its UTM.

In 2014, the company appointed a new CEO and shifted its strategy even more towartelecom operators with LTE cell security. In May 2014, Clavister entered the Stockholnstock market.

Clavister is a good shortlist candidate for municipalities and distributed publiadministration in Northern Europe, or for organization in need of rugged UTM appliances.

Strengths

Clients cite very functional security modules and quality vendor support as reasofor remaining faithful to Clavister.

The ISO 9001:2008 certification and a two-year standard return-and-repair warrantappeal to specific midsize vertical industries or to clients that have experiencehardware issues with other UTM providers in the past.

The Clavister X8 series of rugged appliances is a good alternative for organizationfrom specific vertical industries, such as defense, or when the external conditionwhere the UTM appliance needs to be located are adverse.

Cautions

While Clavister continues to serve the SMB market with software features that were developed in the past, its current go-to-market approach is now primarily focuseon carrier and enterprise needs.

Clavister's sales, support and channel partner resources are focused predominantlon Northern Europe, and might be unevenly available for customers from other regions.

Clavister rarely appears on Gartner clients' shortlists.

Cyberoam

Based in India, Cyberoam, now a Sophos company, is a pure-play vendor for the UTM market, primarily focusing on SMBs and attempting to expand to larger enterprises. Cyberoam provides 18 different UTM hardware models and five virtual appliances. Cyberoam markets its Layer 8 user identity control features as a key differentiator to other UTM products, and ovethe years it has built several features leveraging this concept.

In February 2014, Cyberoam was acquired by Sophos. The company announced that Cyberoam would continue to sell its UTM product line without any short-term disruption. RecenCyberoam updates include features targeting the industrial security use case.

Cyberoam is a good choice for SMB organizations in the Asia/Pacific and Middle Easregions. SMB buyers from other regions should first evaluate local channel expertiseon UTM and customer references with similar use cases.

Strengths

Cyberoam invests heavily on its channel, provides a comprehensive knowledge baseand allows direct access to chat and phone support for its partners that should oftebe translated into quick resolution of support issues for its clients.

Cyberoam consistently executes on its road map.

Cyberoam includes mature embedded reporting and user identity controls that are attractive to midsize organizations.

Cyberoam's filtering policy embeds download and upload statistics for each rule, whichelps determine duplicate and unused rules. It also provides a flexible way to restricrecreational Internet usage with the ability to set up quotas for users or groupsof users.

Cautions

Cyberoam has low visibility in the Americas and appears less often than leading UTMvendors in Europe in competitive shortlists from Gartner clients.

Gartner believes that, while no major change has been observed yet, Cyberoam's channel might suffer in the future from the offensive postacquisition messaging from competitioin Europe and in the U.S., and might be challenged in its home country by local UTMvendors. This could translate in local support disruptions if some channel partnerswitch to other brands.

SMB clients should first obtain clarification from Cyberoam on overlaps between Sophos and Cyberoam's UTM product lines.

Dell

Dell, with headquarters in Round Rock, Texas, is a leading computer manufacturer that has diversified its activity in infrastructure and security. Its UTM portfolio is branded Dell SonicWALL and includes 13 models. It is composed of two product lines that are sold to the SMB market: the SonicWALL TZ Series for the smallest businesses and the SonicWALL NSA Series for small and midsize companies. Despite the recent change in name, Dell's UTM product has been on the market for a long time, and benefits from extended sales and support channels. Dell targets the enterprise market with its SonicWALL SuperMassive Series. Dell also provides other network security solutions, such as SSL VPN and email security gateway.

Dell is a good shortlist candidate for U.S.-based SMBs and for current Dell customers in other regions.

Strengths

- Dell SonicWALL TZ appliances continually get good scores from small organizations for their ability to combine security modules and wireless connectivity, in addition to other network features.
- Clients report that low price and a comprehensive set of features are differentiators for Dell SonicWALL in competitive evaluations.
- Dell leverages its broad logistical capabilities to assist with deployments involving multiple geographies.
- Dell continues to invest in its security divisions, and Dell SonicWALL has a substantial R&D team, including a large in-house security lab that creates all its IPS signatures.

Cautions

- Dell's road map for the past 24 months demonstrates a switch in priority toward enterprise use case at the expense of SMB needs for consolidated network and security features.
- Gartner has observed that since the acquisition of SonicWALL by Dell, many UTM vendors exploit Dell's recent market focus switch and aggressively target Dell's resellers and give them strong incentive to switch. Clients could be affected by a changing relationship between their local channel partner and the UTM technology vendor.
- Dell still holds a good share of the UTM market, but the Dell SonicWALL product line appears much less often in recent UTM shortlists.
- Gartner clients report that the management interface can be confusing because of too many available options.

Fortinet

Fortinet is a large security vendor with headquarters in Sunnyvale, California. It offer more than 40 different UTM appliance models (FortiGate) aimed at the small and midsize market, including wireless, DSL and POE versions. FortiGate is also available as a virtual appliance with five models that are priced based on CPU core count. On-premises centralized management (FortiManager) and reporting (FortiAnalyzer) solutions complement the UTM offering. The comprehensive security product portfolio, composed of tokens and host agents (FortiClient), is designed to appeal to VARs and MSSPs as the route to sales.

Fortinet's road map continues to be driven by regular hardware and software updates with 10 new FortiGate appliances in 2013 and already 12 models in 2014. Fortinet also made FortiGate, FortiManager, FortiAnalyzer and FortiWeb available on the AWS platform. It was also one of the first vendors to offer file sandboxing on a UTM.

Fortinet is a good candidate for every organization in need of a UTM.

Strengths

- Fortinet continues to be a highly visible UTM provider among Gartner clients. It also owns the largest market share, growing faster than the market average, and has the largest base of certified channel partners for UTM technology.
- Fortinet has a very large R&D team and support centers across all regions. Gartner continues to view Fortinet as setting the cadence in the UTM market, driving its competitors to react.
- FortiGate integrates file sandboxing capabilities, backed up by the large FortiGuard Labs threat research team.
- Fortinet provides a very aggressive price/performance proposition, which is often a decisive factor for budget-constrained SMBs.
- The combination of wireless access point management, Wi-Fi analytics, high port density and power on Ethernet along with the availability of price-competitive UTM appliance appeals to small businesses looking for more than a security gateway, as well as to distributed retail organizations.

Cautions

- The frequent hardware and software updates make it more difficult to maintain a consistent level of expertise across Fortinet's widely distributed channel, which sometimes causes discrepancies in presales and support quality.
- Gartner clients report issues related to Fortinet UTM regarding the usability of the FortiManager centralized management, or because of lower than expected performance when enabling security features.
- Fortinet has not yet invested as much as some of its direct competitors in its native cloud-based centralized management and reporting (FortiCloud). While market needs have not fully formed, this will prove a competitive disadvantage if the resellers and MSSPs start to use cloud management as a standard platform.

gateprotect

Germany-based gateprotect is a pure-play security vendor. Its UTM portfolio includes nine appliances. Virtual appliances and centralized management are also available. Gateprotect's management interface (eGUI) implements a graphical (icon-based) visualization of the network topology as a way to simplify the configuration of the security policy. In July 2014 gateprotect was acquired by Rohde & Schwarz, a large German electronics group.

Gateprotect recently released an appliance for small offices (GPO 110), including wireless options and added application and endpoint control features.

Gateprotect is a good shortlist candidate for small organizations, especially in Europe.

Strengths

- Gateprotect's eGUI provides small and distributed organizations with a simplified deployment experience.
- Gateprotect makes a strong investment in R&D for a vendor of its size.
- Clients report that they can get quick answers from vendor support when needed.
- Gateprotect is growing quickly in Latin America and Southern Africa.

Cautions

- Gateprotect has a slower overall growth than most of its direct competitors. Its result still predominantly depend on the mature market of small and lower midsize organization in Germany.
- Gateprotect has limited coverage from independent testing labs.
- Layer 7 application control is not fully integrated in the core view of the graphical security policy representation, but attached as a profile.

Hillstone Networks

Hillstone Networks is a pure network security player, with headquarters in Beijing and operations in Sunnyvale, California. Its UTM portfolio includes 12 hardware models (the M Series). Virtual appliances are not available, but the UTM software can be deployed on an open stack environment. Hillstone does not yet offer a virtual UTM appliance, but several instances of UTMs can run in a single physical chassis. Hillstone also provides a range of firewalls (the X Series) that is specialized for the data center use case

Recent software updates included improvements on VPN, authentication and network features.

Hillstone is a good shortlist candidate for SMB organizations in the Asia/Pacific region. Organizations from other regions should first check the local channel and vendor presences.

Strengths

- Hillstone's UTM includes host reputation and network monitoring features that can help detect infected hosts.
- Clients report that the UTM maintains expected performance when running multiple security modules.
- As a pure-play network security vendor, Hillstone Networks has a good history of execution on its road map, which gives credibility to its announcements on future improvements.

Cautions

- Hillstone targets primarily the large enterprise market. It lags its competitors in automated activity reports for SMB or MSSP operation teams.
- Hillstone Networks is not visible in UTM competitive shortlists outside of China. Half of Hillstone's revenue come from direct sales, and the vendor has yet to build an international channel of active UTM resellers.

Huawei

Huawei is a large network infrastructure supplier headquartered in Shenzhen, China. In 2009, Huawei launched its Unified Security Gateway (USG) product line, which now is composed of 24 models, including a large number of appliances with wireless capabilities, to address the SMB market. Centralized management software is available. Large UTM appliances can run several UTM software instances, but the vendor does not provide virtual UTM appliances to run on the top of leading hypervisors.

Recent updates include new hardware models, a proprietary VPN mode (DSVPN) and SSL decryption.

Huawei's UTM is a good contender for SMBs in China, and for its current large enterprise customers in other countries.

Strengths

- Huawei UTM has a good mix of local certifications and independent tests from large international labs.
- Clients often cite good prices, especially for support service, as a decisive factor in selecting Huawei's solutions.
- Huawei has a large number of clients using IPv6.

Cautions

- Like most infrastructure vendors, Huawei's leverage is in its existing customer base of large enterprises and carriers. This focus on other markets might divert development priorities away from SMB needs.
- Huawei sells a majority of its UTM in China and struggles to grow market share outside of Asia/Pacific. SMB customers should first assess the level of commitment of Huawei's local

channel partners to the SMB market.

Juniper Networks

Juniper Networks is a network infrastructure vendor based in Sunnyvale, California. It has a broad portfolio that covers network and security solutions. Its UTM offering (SRX Series) includes 13 models and relies on the Junos OS, which is the common platform for network and security appliances in Juniper's portfolio. Other product lines can support UTM capabilities (SSG Series and ISG Series), and two virtual appliances are available.

Juniper recently announced a unified centralized management and reporting solution, improved application control engine and simplified user single sign-on.

Juniper UTM is a good choice for existing Juniper customers. Other SMB customers should first verify the experience of their local channel with Juniper security solutions for an SMB use case.

Strengths

- UTM buyers that already use Juniper technology can leverage their existing relationship with the vendor to get a lower price and quickly learn how to manage its UTM.
- Juniper has a broad range of hardware appliances to support a wide variety of scalability and performance requirements.
- Juniper's understanding of diverse customer environments makes it a good choice for complex network infrastructure or when support is a critical component of the purchase decision.

Cautions

- Juniper rarely appears on Gartner SMB customer shortlists for UTM.
- Recent staff cuts in Juniper security teams might divert even more of its resource from the SMB market.
- Except for the support of new hardware models, Juniper has not released new features primarily targeting SMB in the past 12 months.

Sophos

Based in Boston, Massachusetts, and Oxford, U.K., Sophos is a large security vendor that initially provided endpoint security before adding network and mobile security solutions to its portfolio. The Sophos UTM portfolio includes 11 models (the SG Series). Sophos UTM is also available as a virtual appliance on AWS, with a consistent customer base. It also offers its Remote Ethernet Device (RED) appliances for small branches that are centrally managed using a Sophos UTM.

In recent months, Sophos acquired Cyberoam, another UTM vendor (reviewed earlier in this research), started a hardware appliances refresh and released version 9.2 of its UTM software, which includes cloud-based sandboxing, automated email encryption and integration with Sophos' MDM product.

Sophos is a good UTM shortlist contender for SMBs, especially in Europe and Japan and for current Sophos customers. Customers outside of these regions should verify the experience of the local channel for the selected UTM technology.

Strengths

- Sophos' ease of use consistently rates high. The interface contains general guidance on what each feature does, which is useful for SMB operators, who are not all security experts.
- Sophos shows commitment to the UTM market with two recent acquisitions and strong marketing and R&D investment.
- Sophos' UTM community of resellers and clients remains faithful to the brand and contributes to regular spot-on improvements of the technology.
- Sophos support is available in a variety of European languages, and its local presale and support presence received positive scores from Gartner customers.

Cautions

- The integration of Cyberoam's technology will be the main challenge for Sophos during the next 24 months. Gartner believes that, despite some synergies, managing significant overlaps in UTM product portfolios could be difficult for Sophos' channel.
- Sophos UTM's user identity integration and voice over IP (VoIP) management lag behind some of its direct competition.
- Except for Germany and the U.K., Sophos is not as visible in Gartner client inquiries as other Leaders.

Stormshield

France-based Stormshield is a subsidiary of Airbus Defence and Space, and the result of an operational merger between two French firewall vendors in 2013 (Arkoon and Netasq). In addition to firewalls and UTM, the vendor provides endpoint and data security solutions. Its UTM product line (Stormshield Network Security) is made of nine appliances, and seven virtual appliances, and is also available on AWS. Stormshield developed its own IPS, which is enabled in the default UTM configuration.

Recent changes include the branding update, tunnel-based SSL VPN, significant improvement in the URL filtering, embedded reports and log viewer, and single sign-on authentication modules.

Stormshield is a good UTM contender for SMBs in Europe and the Middle East. Other regions should first monitor the availability and experience of the local channel.

Strengths

- Stormshield has a simple service offering with two main bundles: a low-cost bundle and a premium bundle that includes Kaspersky Anti-Virus and vulnerability detection modules.
- Customers like the ease of installation, the integrated rule collision mechanism and the

availability of local and global certifications.

Stormshield's customers will eventually benefit from the larger scale and greateresources of the combined entity. The vendor is starting to be seen as a growing competitivthreat by other UTM vendors in Europe.

Cautions

Despite longtime efforts, Stormshield has not managed to take significant market share outside of France. Europe is a much more fragmented market than North America or other regions with large countries, and as such, requires strong investment for each nevtargeted country outside of the vendor's home market.

Gartner has observed that the Stormshield marketing message and announced road map shifted from SMBs toward large enterprises just after the merger, and that road map execution stalled for a few months. The latest versions now target SMB clients, buSMB buyers should require visibility regarding future road map developments.

Stormshield UTM lacks the ability to apply quality of service (QoS) rules based oapplication detection.

WatchGuard

Seattle-based WatchGuard is a well-established UTM vendor. It provides UTM, secure email gateways and remote manageable wireless APs. The UTM product lines (XTM and Firebox), include 19 physical appliances, including three appliances with embedded wireless capabilities and four virtual appliances.

WatchGuard recent releases include a new cloud-based reporting and monitoring solution (WatchGuard Dimension), a DLP as well as cloud-based sandboxing modules, and wireleaccess point management.

WatchGuard is a good shortlist candidate for SMB organizations in need of a broaset of features or relying on an MSSP for managing and monitoring their UTM.

Strengths

WatchGuard provides cloud-based sandboxing (APT Blocker), and reports are directly integrated in its centralized dashboard cloud service (WatchGuard Dimension).

WatchGuard's customers indicate that completeness of features and low price are reasonto select WatchGuard.

WatchGuard has demonstrated a strong ability to execute on its road map, leveragin its platform modularity to quickly add new modules.

The WatchGuard Dimension reporting tool includes an interactive heat map view (FireWatch) that is useful to quickly identify network issues created by a specific user or application.

Cautions

WatchGuard appears more rarely in Gartner client shortlists for midsize or distributed organizations than its direct competitors.

Gartner does not see WatchGuard displacing other Leaders based on technical requirements.

Clients report that the on-premises centralized management console for WatchGuaUTMs could be improved.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes amarkets change. As a result of these adjustments, the mix of vendors in any MagiQuadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadranor MarketScope one year and not the next does not necessarily indicate that we havechanged our opinion of that vendor. It may be a reflection of a change in the marketand, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

Aker Security Solutions, Hillstone Networks and Barracuda Networks have been added.

Dropped

Kerio was dropped because it did not meet Gartner's inclusion criteria for this MagiQuadrant.

Inclusion and Exclusion Criteria

Inclusion Criteria

UTM companies that meet the market definition and description were considered fothis report under the following conditions:

They shipped UTM software and/or hardware products — targeted to SMBs — that included capabilities in the following feature areas at a minimum:

- Network security (stateful firewall and intrusion prevention)
- Web security gateway
- Remote access for mobile employees (VPNs)
- Email security

They regularly appeared on Gartner midsize-client shortlists for final selection.

They achieved UTM product sales (not including maintenance or other service feesof more than $7 million in 2013, and within a customer segment that's visible to GartnerThey also achieved this revenue on the basis of product sales, exclusive of managesecurity service (MSS) revenue.

The vendor can provide at least three reference customers willing to talk to Gartnefor

Gartner has had sufficient input from Gartner clients on the product.

Exclusion Criteria

There was insufficient information for assessment, and the company didn't otherwise meet the inclusion criteria or isn't actively shipping products yet.

Products aren't usually deployed as the primary, Internet-facing firewall (for example — proxy servers and network intrusion prevention system [IPS] solutions).

Products are built around personal firewalls, host-based firewalls, host-based IPS and Web application firewalls — all of which are distinct markets.

Solutions are typically delivered as MSS, to the extent that product sales did not reach the $7 million threshold.

In addition to the vendors included in this report, Gartner tracks other vendors that did not meet our inclusion criteria because of a specific vertical market focus and/or UTM revenue and/or competitive visibility levels, including Adyton Systems, eSoftGaj Shield, ilem Group, My Digital Shield, Netgear, North Coast Security Group, QuickHeal, Sangfor, SecPoint, Secui, Smoothwall, Trustwave and ZyXEL.

Evaluation Criteria

Ability to Execute

Product or Service: Key features — such as ease of deployment and operation, console quality, price/performance, range of models, secondary product capabilities (including logging, mobile device management, integrated Wi-Fi support and remote access), and the ability to support multifunction deployments — are weighted heavily.

Overall Viability: This includes a vendor's overall financial health, prospects for continuing operations, company history, and demonstrated commitment to the multifunction firewall and network security market. Growth of the customer base and revenue derived from sales are also considered. All vendors are required to disclose comparable market data, such as multifunction firewall revenue, competitive wins versus key competitors (which is compared with Gartner data on such competitions held by our clients), and devices in deployment. The number of multifunction firewalls shipped isn't a key measure of execution. Instead, we consider the use of these firewalls and the features deployed to protect the key business systems of Gartner midsize-business clients.

Sales Execution/Pricing: This includes pricing, the number of deals, the installed base, and the strength of sales and distribution operations of the vendors. Presales and postsales support are evaluated. Pricing is compared in terms of a typical midsize-business deployment including the cost of all hardware, support, maintenance and installation. Low pricing won't guarantee high execution or client interest. Buyers want value more than they want bargains, although low price is often a factor in building shortlists. The total cost of ownership during a typical multifunction firewall life cycle (which is three to five years) is assessed, as is the pricing model for adding security safeguards. In addition, the cost of refreshing the products is evaluated, as is the cost of replacing a competing product without intolerable costs or interruptions.

Market Responsiveness/Record: This includes the ability to respond, change direction, be flexible, and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the provider's history of responsiveness.

Marketing Execution: This addresses awareness of the product in the market. We recognize companies that are consistently identified by our clients and often appear on their preliminary shortlists.

Customer Experience and Operations: These include management experience and track record, and the depth of staff experience — specifically in the security marketplace. The greatest factor in these categories is customer satisfaction throughout the sales and product life cycle. Also important is ease of use, overall throughput across different deployment scenarios, and how the firewall fares under attack conditions (see Table 1).

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Low
Customer Experience	Medium
Operations	Medium

Source: Gartner (August 2014)

Completeness of Vision

Market Understanding and **Marketing Strategy:** These include providing a track record of delivering on innovation that precedes customer demand, rather than an "us, too" road map and an overall understanding and commitment to the security market (specifically the SMB network security market). Gartner makes this assessment subjectively by several means, including interaction with vendors in briefings and feedback from Gartner clients on information they receive concerning road maps. Incumbent vendor market performance is reviewed yearly against specific

recommendations that have been made to each vendor, and against future trends identified in Gartner research. Vendors can't merely state an aggressive future goal. They must enact a plan, show that they're following it and modify the plan as they forecast how market directions will change.

Sales Strategy: This includes preproduct and postproduct support, value for pricing, and clear explanations and recommendations for detection events and deployment efficacy. Building loyalty through credibility with a full-time midsize-business security and research staff demonstrates the ability to assess the next generation of requirements.

Offering (Product) Strategy: The emphasis is on the vendor's product road map, current features, leading-edge capabilities, virtualization and performance. The quality of the security research labs behind the security features is considered. Credible, independent third-party certifications such as Common Criteria, are included. Integration with other security components is also weighted, as well as product integration with other IT systems. As threats change and become more targeted and complex, we weight vendors highly if they have road maps to move beyond purely signature-based, deep packet inspection techniques. In addition, we weight vendors that add mobile device management to their offerings and are looking to support SMB organizations that use cloud-based services.

Business Model: This includes the process and success rate of developing new features and innovation, and R&D spending.

Innovation: This includes product innovation, such as R&D, and quality differentiators, such as performance, virtualization, integration with other security products, a management interface, and clarity of reporting.

Geographic Strategy: This includes the ability and commitment to service geographies.

The more a product mirrors the workflow of the midsize-business operations scenario the better the vision. Products that aren't intuitive in deployment, or operation that are difficult to configure or have limited reporting, are scored accordingly. Solving customer problems is a key element of this category. Reducing the rule base, offering interproduct support and beating competitors to market with new features are foremost (see Table 2).

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	High
Sales Strategy	Medium
Offering (Product) Strategy	Medium
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Low

Source: Gartner (August 2014)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors at the forefront of making and selling UTM product that are built for midsize-business requirements. The requirements necessary for leadership include a wide range of models to cover midsize-business use cases, support for multiple features, and a management and reporting capability that's designed for ease of use. Vendors in this quadrant lead the market in offering new safeguarding features, and in enabling customers to deploy them inexpensively without significantly affecting the end-user experience or increasing staffing burdens. These vendors also have a good track record of avoiding vulnerabilities in their security products. Common characteristics include reliability, consistent throughput, and products that are intuitive to manage and administer.

Challengers

The Challengers quadrant contains vendors that have achieved a sound customer base but they aren't leading with features. Many Challengers have other successful security products in the midsize world and are counting on the client relationship or channel strength, rather than the product, to win deals. Challengers' products are often well-priced and, because of their strength in execution, these vendors can offer economic security product bundles that others can't. Many Challengers hold themselves back from becoming Leaders because they're obligated to set security or firewall products as a lower priority in their overall product sets.

Visionaries

Visionaries have the right designs and features for the midsize business, but lack the sales base, strategy or financial means to compete globally with Leaders and Challengers. Most Visionaries' products have good security capabilities, but lack the performance capability and support network. Savings and high-touch support can be achieved for organizations that are willing to update products more frequently and switch vendors, if required. Where security technology is a competitive element for an enterprise, Visionaries are good shortlist candidates.

Niche Players

Most vendors in the Niche Players quadrant are enterprise-centric or small-office-centric in their

approach to UTM devices for SMBs. Some Niche Players focus on specific vertic industries or geographies. If SMBs are already clients of these vendors for othe products, then Niche Players can be shortlisted.

Context

SMBs have significantly different network security requirements from those of larg enterprises, due to different threat environments and different business pressures Although the branch offices of some larger enterprises have requirements that are similar to midsize businesses, this is not always the case. The UTM market consists of a wide range of suppliers that meet the common core security requirements of SMBs, but businesses need to make their decisions by mapping their threat and deployment patterns to optimal offerings.

Market Overview

The UTM market is mature and many SMB organizations are now renewing their UTM technology, rather than acquiring it for the first time. The market is still growing faster tha other network security markets, but higher market penetration will slowly drive the UTM market growth rate down. In 2014, Sophos acquired Cyberoam, continuing the recent trend of consolidation in the UTM market.

The primary characteristic of midsize companies is that they are organizations wit resource-constrained IT departments. They have a relative limit on capital expenditures operational budgets, number of IT staffers and depth of IT skills when compared with large enterprises. In keeping with this, UTM appliances are frequently used across midsize businesses as a low-cost way of meeting their network security requirements. Midsize businesses look at security differently, and show different buying behaviors compared with larger enterprises. The primary areas of difference are (in order of importance):

- A limited or nonexistent skilled security staff drives the need for ease of installation, configuration and use of channel-managed solutions.
- Less complex use of the Internet results in lower demand for high-end security features such as application-level security and custom intrusion prevention filters.
- Limited security budgets drive acquisition costs to represent more than 60% of the overall decision weighting.
- Small businesses often perceive that they are not visible to attackers and, therefore don't require as much security. However, financially motivated attackers have targete small businesses, and the publicity over successful attacks has changed these businesses' perceptions.

Small businesses with fewer than 100 employees have even more budgetary pressure and even fewer security pressures. Most security procurement decisions are drive by nontechnical factors and rarely feature competitive comparisons. For these reasons this Magic Quadrant focuses on the UTM products used by midsize businesses, as defined above.

These differences between SMB and large-enterprise expectations are one of the major reasons why many of firewall vendors that sell successfully to the enterprise an SMB markets tend to have separate software or even product lines for each market.

UTM Vendors Target Large Enterprises With Different Approaches

All of the vendors surveyed agree on the different go-to-market approaches when targetin SMBs versus large-enterprise clients. SMBs more often rely on their channel partne to choose the correct all-in-one UTM platform, whereas large-enterprise security buyer conduct their own selection process. SMB resellers also handle Level 1 and Level 2 support; some also become local Level 3 support centers on behalf of the vendor.

The market penetration for SMBs is high, and displacing active channel partners fro another UTM vendor is difficult because it means these partners will have to maintai the legacy technology of existing customers, and also learn the vendor's replacement technology. Even if some channel displacement happens following an acquisition or merger announcement, Gartner observes that many UTM vendors consider SMBs as a mature, low-growth market and focus on new target customers.

The most basic tactic is to release more powerful appliances, run the same softwar stack and sell the UTM core value of all-in-one security. This shortsighted approac dooms the vendors to niche use cases, such as budget-constrained lower-size large enterprises, which are composed of slightly more than 1,000 employees. Some of the larger UTM vendors improve on this initial approach with an optimized software stack that is developed to provide an enhanced offer for the use case of a high-performance firewall. Despite the management interface being crowded with unnecessary features, the good price offered by vendors that are aggressively willing to take market shar away from the incumbent enterprise firewall vendors is attractive to many enterprises However, UTM vendors that do not take a more differentiated product approach won' displace leading enterprise vendors at large, Type A organizations (see "Magic Quadrant for Enterprise Network Firewalls").

Alternatively, a few providers now target distributed organizations that have need close to those of midsize organizations. This includes MSSPs for SMBs and distribute enterprises like retailers, health organizations and small governmental agencies Despite centralized purchase and maintenance centers, each office is similar to an autonomous organization. Recently released offers include centralized cloud-based management and reporting and wireless access point management, sometimes with additional features targeting organizations from the retail industry, such as wireless analytics, but also smaller appliances of less than $500.

UTM vendors increasingly are fighting over initial purchase prices, and all vendor manage to win deals on the strength of this sole advantage, based on the targete vertical and geographic area. In the longer term, the security market for SMB might be influenced by the increased adoption of mobile technology, cloud services and —for upper midsize businesses — virtualized demilitarized zone (DMZ) and data center. While there is no visible actor that could disrupt the UTM market yet, alternate approaches, such as endpoint and mobile device management or secure Web gateway

hosted in the cloud, could become more serious contenders.